PRIVACY AND INFORMATION SYSTEMS: AN ARGUMENT AND AN IMPLEMENTATION

J. J. Hellman

May 1970

PRIVACY AND INFORMATION SYSTEMS: AN ARGUMENT AND AN IMPLEMENTATION

J. J. Hellman, Consultant*

The RAND Corporation, Santa Monica, California

ABSTRACT

This thesis is presented in two parts. The first examines the social and technical implications of information systems vis à vis the individual's ability to control the dissemination of information about himself. We argue here that information systems must incorporate certain properties in their initial design in order to safeguard man's individuality while still providing a complex and interdependent society the information it needs to function effectively. These properties are:

1) Control of access by the individual;
2) Accuracy and completeness of information;
3) Audit trail;
4) Potent legislative support.

The philosophy embodied by these properties is meant to guide the evolution of technology. In that respect they are implementation independent.

The second part of this thesis applies these properties of safe information systems derived in Part I to problems currently encountered in the medical environment. A toxicological information system, a drug information system, and a patient's medical record information system are each analyzed vis à vis society's right to learn and the individual's right of privacy. The framework for this discussion is presented in Part I--the dual role of man. Suggestions are then presented for using available techniques to safeguard society's attempts at using the new information handling technologies (computers).

---

*Any views expressed in this Paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

This Paper, by J. J. Hellman, a RAND Corporation Consultant, has been submitted as a Master's thesis at MIT.

PREFACE

The idea for this study developed as a result of my working on an information system for the office of the Graduate School of Electrical Engineering at MIT. After developing an on-line system containing sensitive information on identifiable individuals, I became interested in the privacy and confidentiality issues surrounding this project. Consequently, I began the research reported here.

In Part I, I am concerned with the philosophical underpinnings and the resultant policy implications of these issues. The time scale is necessarily large. In Part II, however, I focus on current problems encountered in the medical environment and apply the policies derived in Part I in terms of current technology.

CONTENTS

PART II

MEDICAL INFORMATION SYSTEMS AND THE PROTECTION OF PRIVACY

FIGURES

PART I

ON THE NECESSITY OF PERSONAL CONTROL OF PERSONAL INFORMATION

The right to privacy is the right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and facts of his personal life. It is a right that is essential to insure dignity and freedom of self-determination.

—Paul Armer

Social Implications of the Computer Utility

I. INTRODUCTION

The computer offers mankind the opportunity to exercise more effective control over his environment through its ability to handle large amounts of information both accurately and speedily. If put to proper use, information could be disseminated to the right people at the right time. However, the current trend towards the agglomeration of data on individuals, via the computer, presents a serious threat to the individual's right to privacy. If allowed to proliferate, the deleterious effects on the individual, and therefore society, are likely to be irreparable. This first part of the thesis examines some social and technical implications of information systems vis à vis the individual's ability to control the dissemination of information about himself. It is argued here that information systems need incorporate certain properties in their initial design in order to safeguard man's individuality while still providing a complex and interdependent society the information it needs to function effectively.

Because of the *momentum of technology* and the *irreversibility* of social processes, society must act immediately if it is to ensure the evolution of "safe" information systems. The very nature of information itself makes the price of failure prohibitive. Once "stolen" (revealed) it can never be returned; nor can the resultant damage be objectively valued. On the contrary, the value of personal information to the

individual concerned is by definition subjective. Therefore, properties providing the individual his rightful control over the dissemination of personal information must be inherent in any personal-information system.

II. PRIVACY

In asserting the paramountcy of the individual, the Declaration of Independence cites man's inalienable rights as life, liberty, and the pursuit of happiness. Professors Fried [1] and Westin [2] posit that a necessary condition for the individual to retain these rights is the strict enforcement of the right to privacy. Samuel D. Warran and Louis D. Brandeis, in "The Right to Privacy," trace the common-law evolution of this right:

> . . . now the right to life has come to mean the right to enjoy life--the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession--intangible, as well as tangible [3].

Privacy is a fundamental right; without it, the individual becomes subservient to the state, and the notion of participatory democracy becomes mere rhetoric.*

A PERSONAL-INFORMATION SYSTEM

A personal-information system consists of four functional components, *people*, *users*, *management*, and *technology*. The people are the set of individuals who have certain information about themselves stored in the system. The users are

---

*A scenario of a society that does not respect this right to privacy is constructed by Professor A. Westin in "The Snooping Machine" [4]. George Orwell's *1984* is another characterization of a society that places little value on the sanctity of the individual.

the set of individuals or organizations that have need to reference the data base in the normal course of their work. The management are the set of individuals who, functioning as a unit, have the responsibility to collect, update, and process the information contained in the data base. (Historically, the users and the management are the same set of individuals.)

The inertia of that now obsolete clerk filing-cabinet system of information processing was sufficient to make the pooling of information and the executing of inferential retrievals virtually impossible. Organizations were hard pressed to process the information they needed in daily operations. With the development of the computer, however, the notion of centralizing information has become attractive. As a result, the management and users would function as independent components.

The most important characteristics of the management of an information system are their potent ability to access the data base coupled with the lack of permission to do so. The management's sole responsibility is to insure the efficient operation of the facility; the actual content of the data base is irrelevant to performance of duties.

THE PROBLEM

Substantial pressures exist to apply the new information (computer) technologies to the problems confronting organizations. Evidence of this fact is the spontaneous growth of

computerized data banks [5,6]--the credit bureaus, corporate personnel files, Federal bureaus, etc. In order to comprehend the crucial issues, and thereby arrive at a viable solution to the problem of maintaining the sanctity of the individual while exploiting the new powers given to society in the computer, one should investigate relevant aspects of the nature of *technology*, *society*, *man*, and *organization*.

III. THE NATURE OF TECHNOLOGY

The development of new technologies enables man both to better perform already feasible tasks (where better is defined in terms of time, money, etc.), and to perform a new set of tasks that were heretofore infeasible. Technology provides man with apparatus that augment his ability to interact with his environment. For example, the microscope enables man to see minute objects, the bulldozer enables man to move massive objects, and so on. Thus, technology is intrinsically an "amplifier." If used properly, technology expands man's ability to perform desirable tasks. If misused, however, the extent of the damage to society is similarly magnified.

TECHNOLOGY AND SOCIETY

> The primary effects of technological progress on society are the opening up of new opportunities and the lessening of existing constraints on human activities. The new opportunities and the lesser constraints perturb the existing equilibrium on the operation of society and trigger a process of evolution toward a different mode of operation consistent with the new technological environment. The resulting changes in society are the most important effects of technological progress, yet their character depends largely on social forces and goals unrelated to the technological developments that initiated them [7].

Technological evolution has reduced the "size" of the world and increased the complexity of social structures. No longer do individuals function as self-sustaining units. Rather, as a consequence of an evolving technology, man finds himself forced to specialize. Thus, in order to satisfy

certain basic needs, such as earning a living, man has to coordinate his efforts with other specialists. To enhance the efficiency of this cooperation, organizations were formed. The increased complexity of these structures (organizations), in turn, forces greater emphasis on specialization. As a result, further emphasis is placed on the development of new technologies to make these structures function even more efficiently.

When organizations were forced to specialize, they became the functional units in an even more complex social structure.

Figure 1 models this feedback relationship:

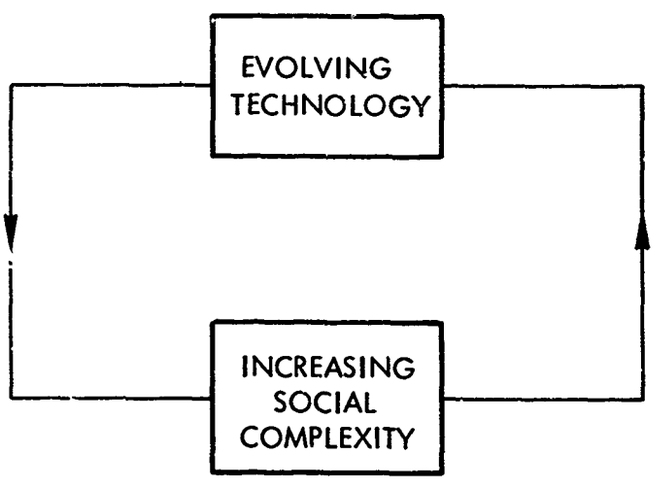

Fig. 1--Technological/Social Complexity Feedback Structure

IV. SOCIETY AS A COMPLEX FEEDBACK SYSTEM

In today's society, events occurring in one part of the world often have substantial effects in other parts of the world. These effects may culminate in actions which then affect other areas, perhaps including the one where the original event occurred. The range of effects of these reactions is of such proportions that their existence cannot be ignored. The significance of this complex feedback nature of society and its dependence on technology is illustrated by the operation of the financial exchanges. News from all over the world continually flows into the various exchanges. Reports of events of every conceivable nature and origin comprise the content of this information. Investors analyze these latest communications and modify their attitudes accordingly. These attitudes then translate into actions. As a consequence, the prices of various commodities vary. These price variations, in turn, are of vital concern to the governments and large corporations whose actions often affect the world situation.

Thus, through the complex mechanism of the marketplace, events occurring in one part of the world often have substantial and unpredictable effects on other parts. Surely, such a marketplace structure could not have evolved if transportation systems for the distribution of goods were nonexistent. Neither would it have been able to function if communications networks were not developed.

V. THE DUAL ROLE OF MAN

The pursuit of happiness in today's society compels man to assume two functional roles, concurrently:

1) Man as an individual.

2) Man as a member of organizations.

As an individual, man demands to be autonomous. In order that he be at peace with himself and society, he must feel that he has control over his own destiny. In this role, man needs to be a private entity.*

In his second role, man acts to ensure that his organization functions as efficiently as possible, entirely natural because man created the organization as an effective means of satisfying certain of his personal needs.† Thus, the pressures to develop new technologies for handling the problems confronting organizations are originated by individuals.

---

*"The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual . . ." [3].

†"A corporation is simply an organized body of men acting as a unit, and with a will that has become unified through the singleness of their purpose" [8].

VI. THE CURRENT STATE OF AFFAIRS

As a result of increasing size and complexity, organizations are confronted with an enormous expansion of data gathering and record keeping. The ability to handle this information more effectively would obviously facilitate their operations. The newly developed, rapidly evolving, information (computer) technologies, which enable man to better perform retrievals and sorting of information and to perform inferential retrievals only possible through the agglomeration of large amounts of data, offer the capabilities needed to cope with these information processing problems.

Already, many organizations have computerized their personnel files. The credit bureaus have an information system containing highly sensitive dossiers on approximately 110 million individuals [6]. The application of computer technology to these and many other private and government organizations has catapulted the issue of privacy and the control of personal information from an "academic" problem to an urgent pragmatic one.

VII. THE NATURE OF SOCIAL PROCESSES

Due to the complex feedback nature of society and the amplification property of technology, the range of effects of any single decision is extensive and the effects unpredictable. Many system failures are a result of the control mechanism's failure to function adequately at the proper time. Two significant characteristics of the system under discussion warrant careful consideration: *momentum of technology* and the *crisis* nature of society.

The *momentum of technology* is such that the ability to perform new tasks generates pressures to exploit these new capabilities.* These available technologies then bias the structure and character of organizations.† The organizations exert pressures to further develop those technologies, thereby becoming more deeply entrenched in their present mode of behavior. It would therefore behoove society, specifically

---

*"The issue is not whether Congress will adapt to this (information handling) potential (of the computer) but at what speed" [9].

†". . . the structure and operation of human organizations are likely to be very different in an information-rich society. Perhaps the primary reason why we have to resort to hierarchical control in human organizations is that spontaneous coordination of activities would require more effective information flow than can be achieved today. The question is often asked whether computers will lead to more centralization or decentralization. Our children will probably view such a question as naive because the terms will no longer be relevant" [10].

the architects of computing technology, to create a technology that would effectively foster the growth of desirable systems (organizations) [11].

The block in Fig. 2 labeled "information system" is that subset of a personal-information system comprised of the technology (i.e., the computer) and the actual information (the data base). This unit, if misused by those in a position to control it (referred to here as the management), tends to increase their power, enabling them to further misuse it.

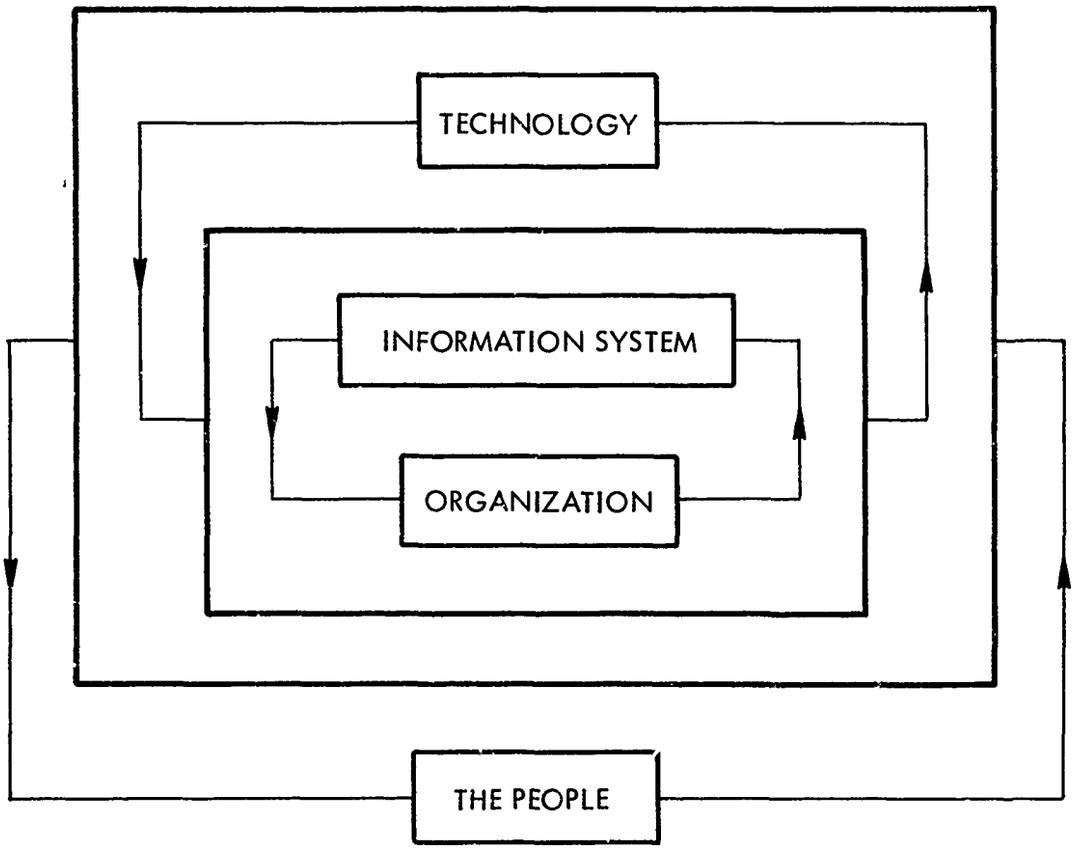

Fig. 2--The Nature of Social Processes

The dominant characteristic of the control loop, at least as shown in the past, is the crisis nature of society. Before society will take any actions to control the system it is monitoring, the perturbations will have to be of crisis portions. Perhaps the most obvious example of this phenomenon is environmental pollution. Before any substantive moves toward control of pollutants are taken, society may well have to be choking--literally. That this is indeed the normal mode of behavior is also attested to by the fact that only after a series of disastrous fires were electrical codes created [12].

AN IRREVERSIBLE PROCESS

> . . . organizations are technical instruments, designed as means to definite goals. They are judged on engineering premises; they are expendable. Institutions, whether conceived as groups or practices, may be partly engineered, but they have also a "natural" dimension . . . they are less readily expendable [13].

Any process requiring the continued efforts of large numbers of people develops certain forms of inertia. These organizations become institutionalized and self-perpetuating. The reason for this phenomenon are functions of the nature of man. Pride in one's work, the need to feel socially useful, create certain attachments between the individual and his work. His work becomes an extension of himself.

If, after a certain length of time, society begins to view particular endeavors as undesirable or simply no longer necessary, the individuals within the organization affected

are likely to feel *personally* attacked. Thus, those individuals may attempt to protect their organization (themselves) in any way they can. Often, the dislocation from an economic point of view is substantial enough to discourage society from changing the *status quo*;* not to mention the effect of reactions vis à vis personal insecurities resulting from a forced reorientation.

Woe to the individual who attempts to question social priorities and the behavior of the organization. Witness the outrageous, illegal investigation of Ralph Nader's private life by General Motors when he questioned their concern for safety:

> A private detective who investigated Ralph Nader, the critic of automobiles as unsafe, has sworn in court papers that General Motors altered and suppressed documents showing that the real purpose of the investigation was to "discredit" Mr. Nader and "Shut him up" . . . The investigation was ordered (by G.M.) after the publication of Mr. Nader's book "Unsafe at Any Speed" [14].

Another organization guilty of heinous trespasses on individual rights, and exploiting to the fullest the power of its resources to protect its autonomy, is the Internal Revenue Service. These facts were revealed in a Senate subcommittee investigation headed by Senator Edward V. Long. In "Big Brother in America," Senator Long writes:

---

*Witness the problems confronting society vis à vis "the military-industrial complex" concerning the redirection of the economy.

The people who reported the most flagrant violations of their rights were those who by their own reports had fought these abusive tactics--taxpayers who had refused to compromise when presented with what they considered unjustified assessments; lawyers who had brought suit in Federal Court to enjoin illegal and improper treatment of their clients; in short, people who had stood up to Big Brother. This penchant for revenge was to prove far more prophetic in our probe than we realized [15].

VIII. EFFICIENCY OR PRIVACY

Apparently, a conflict of interests exists between the organization's desire for efficiency and the individual's demand for privacy. If viewed in the proper perspective, the dual role of man, this apparent conflict between the organization and the individual is in fact internal to the individual, suggesting that the solution lies in an analysis of the goals of the individual.

The most obvious characteristic of these goals is that they are subjective. The Bill of Rights, Declaration of Independence, etc., constitute a set of fundamental rights that allow each person to live by his own set of values and still participate in society as he sees fit. Thus, historical precedent provides the solution to this problem.

Our history is one of attempting to achieve order NOT at the price of liberty, hence the biasing, in favor of the individual, of our system of jurisprudence. Society long ago made the decision that it would rather free a guilty man than imprison an innocent one.* The resultant loss of efficiency was considered a small price to pay compared to the alternative.

Even our democratic political system is intrinsically less than a dictatorship. The time delays due to internal dissent only seem to increase inefficiency. Viewed in this light,

---

*The burden of proof is on the state; the individual is *presumed* innocent until *proven* guilty.

one wonders about the true import of "efficiency." What are the dimensions it is measured in? Is it an end in itself or simply a means to an end? What is the price of efficiency? Given our form of government and the structure of our legal system, it is clear that society places a greater value on the sanctity of the individual than on efficiency.

THE ROLE OF SOCIETY

Personal-information systems exist as an operating convenience. Because of size and complexity, organizations can no longer deal with individuals on a person to person basis. In order to expedite their daily business, information systems containing the pertinent information are utilized. Individuals, understanding the necessity for these systems, voluntarily expose certain facts of their personal lives. But they do not give this information to the managers of the system unconditionally; on the contrary, it is loaned under an implied *contract* that it be used for only certain specific purposes mutually agreed upon. Any use of this information without the express permission of the owner constitutes a violation of the original contract [16,17,18].

At the present time, there are no mechanisms, legal or technological, through which an individual can control the dissemination of this information. Once he has divulged certain facts of his personal life, his privacy is at the

mercy of those now in possession of said information [19]. That this is a most unfortunate and uncomfortable predicament to be in is attested to by the following realities:

1) . . . IRS has for many years been showing so-called confidential tax returns to 23 other Federal agencies, to agencies of all 50 states, and believe it or not, to over a dozen foreign countries! [15,20]

2) On the March 17, 1969 Walter Cronkite show, presented on the Columbia Broadcasting System, it was once again demonstrated that non-credit-granting firms can obtain credit records on individuals [21].

3) . . . Now he has innocently been hurt and put to a tremendous burden, simply because they (the credit bureaus) either have incompetent people or sloppy people, or the system is sloppy. I am convinced that this is rampant throughout the entire credit reporting system. . . . It seems to me if we would change the client relationship, the credit bureau could not give out any information without the express permission of the client, and second. . . . I would have the right to see the record and to correct it before it went out. . . [5].

Until the advent of the computer, this deficiency, the lack of individual control, did not pose too serious a threat to the privacy of the individual. He was protected *de facto* by the inertia of human filing systems and the necessary decentralization of information. In addition, the extent of the information that could be processed was limited. The centralization of information, now feasible as a result of the computer's ability to handle considerable amounts of information at incredible speeds, presents a very real threat to the privacy of the individual.

Every argument used to convince society of the benefits of any system derives its substance from the added power of

new technologies. The greater the extent of the benefits society can accrue if the system is used properly, the greater the cost to society if the system is misused. Since knowledge is power, the potential dangers of this system are indeed awesome [7,4]. As has already been shown, due to the irreversibility of social processes, society cannot afford to wait for evidence of undesirable behavior before it acts [11].

IX. THE PROPERTIES OF A PERSONAL-INFORMATION SYSTEM

Since personal information is at all times the "property" of the individual it describes, the control of its dissemination belongs to the individual alone. That he is willing to aid the operations of society by allowing part of it to reside in an information system does not imply he no longer wants or needs to control its publicity [19]. Therefore, in order for society to benefit from computer technology and yet minimize the risk of misuse, certain properties must be incorporated into the initial design of these systems. These features are implementation independent; the mix of procedural and technical devices will evolve with experience and technology. The philosophy embodied by these properties, however, is designed to direct the evolving technology, ensuring safe growth.

ACCESS CONTROL

Access control must be a technological capability of the system. The individual must have absolute control over the dissemination of his personal information. There is also the problem of joint ownership of information, e.g., medical records, where two individuals would have authority over its publicity. Therefore, the system must provide some mechanism for controlling the access to that type of information. However, the exact implementation is beyond the scope of this Paper.

The individual must be able to specify:

1) Who is allowed to access his file.

2) What parts of it each person is allowed to see.

3) The conditions under which the above may be executed (a "need to know" criteria).

These specifications must be technically implemented because of the nature of society. *Trust* relationships exist only on an individual basis [1]. Thus, no philosophical justification exists for "trusting" the *management of the system*. With regard to protection and *trust*, Professor Westin has written "the system can still be beaten by those in charge [the management] of it, from the programmers who run it, and the mechanics who repair breakdowns to those who are in charge of the enterprise and know all the passwords. This means that a package of legal controls is absolutely essential" [4]. It would violate all principles of our society to place the management of the system in such a position whereby, at their discretion, information to which they are not privileged would be exposed.

There can be no safe data banks unless the state of the art of computer technology is able to control release of information.* Otherwise, the individual will not be properly

*"The threat to privacy is real indeed, but the (Congressional) committees seemed to have missed the point that the threat exists regardless of the establishment of the National Data Center; the fact is that computers can communicate with one another and the physical location of the data is largely immaterial" [7].

protected from illegal invasions of privacy on the part of the management of the system. In the short term it is possible of course, to achieve the protection of privacy through close regulation and tight management. But if relied on for long, the price society would have to pay--an "information gap"--would be dear [7].

ACCURACY AND COMPLETENESS

> Perhaps the safety of a computer system should be certified in the same way that the safety of bridges and buildings are certified and periodically checked. We should keep in mind in this respect that much more than privacy is involved. For instance, unauthorized deletion or modification of information and changes to programs may have more damaging effects to an individual than an invasion of his privacy [10].

A necessary complement to the Access Control property is a mechanism by which the individual can:

1) Verify the accuracy of the information pertaining to him.
2) Change, append, or delete those items of information that warrant such modification.

These items require the creation of a review mechanism whose duty it is to adjudicate matters of information content. Unlike today's courts, these review mechanisms must act without delay. Since computers hasten the flow of information, the time factor is of utmost importance. In the interim, to protect the individual from harm as a result of incomplete or inaccurate information, the system must not allow retrievals of information whose validity is being contested, an extension

of our legal ethic that a man is innocent until proven guilty.

AUDIT FACILITY

The information system must maintain a complete audit trail. This record would be accessible to both the individual and the management. Contained in this record would be information concerning the identity of those individuals requesting access, when and why access was requested, and if it was granted.

Prior to the "information explosion," when individuals or organizations were in need of certain facts pertaining to an individual, they would contact him personally. If the individual felt that the information they requested was uncalled for, he could refuse to give it to them. At the same time, he was well aware of who was interested in him and why. There is no reason why the individual should feel compelled to sacrifice this necessary control over his life.

Some may argue that implementing these properties would be expensive. Every design engineer is well aware of the fact that safety mechanisms cost money. But society has found, in many instances, that the cost of a safety device is small when compared to the cost of the bad outcome. If one but hesitates for a moment to consider how much one is willing to pay for protection against undesirable possibilities, then these safeguards will be demanded. For example, it costs

money to use fuses in an electrical system. Automobile insurance is indeed an expensive safeguard, but few would claim that it is an unnecessary cost.

LEGAL STRUCTURE

> Any proposed bill creating a legal right of privacy should include both a criminal penalty for violation and a civil remedy for damages for injuries resulting from each violation. Consideration should also be given to a waiver of the system's immunity for the torts of its employees who wrongfully breach the privacy of individuals in the course of their employment. . . . Violators should be barred from use of the system in the future [16].

A certain legal structure is needed to create the necessary environment to foster the development of desirable systems. First, society must immediately declare its refusal to tolerate the construction of potentially dangerous systems. That means, any system that does not have the aforementioned properties intrinsic, cannot begin to or continue to operate (viz., credit bureaus, IRS, FBI, the Census Bureau, corporate systems, etc.). A legal structure is called for that both cites illegal acts and holds individuals accountable for their own actions. In order to clarify and support its position on the status of the information in these systems, society must enumerate those acts it considers trespasses on the rights of the individual. Specifically, anyone tampering with the individual's control over the dissemination of his *personal information* would be guilty of a crime against society (violating the information system), and breach of

contract (concerning the individual involved). That legal action is necessary is seen in the unscrupulous activities of the IRS:

> One of the principal sources of nourishment for Big Brother has been the fact that the government agents who have been his most dangerous bully boys have been operating with the comforting knowledge that they themselves won't be held responsible for their actions. This was certainly the case when the Commissioner of the Internal Revenue Service refused to identify the author of the "brainwash" memorandum [15].

X. SOCIAL AND TECHNICAL IMPLICATIONS

The state of the art of computer technology is rapidly approaching the feasibility of the multi-access computer utility [22]. Whether or not remote access terminals will become as common in the future as the telephone is today, may be a function of what society does today. Essentially, society is faced with (when modeled in the extremes) what appears to be a binary choice:*

1) Construct general purpose computer utilities of use to the public. The availability of terminals would provide the mechanism needed to implement the properties previously derived.
2) Allow organizations to monopolize the use of the computer technology, which would result from the economic infeasibility of widespread computing facilities.

Since knowledge is power, the most probable consequences of the second alternative is that the few able to handle large amounts of knowledge effectively will assume positions of power. The mass of society will become ever further removed from the decision-making process.

---

*". . . the nature of the impact (of computers on society) will depend largely on how all of us as individuals and society as a whole will choose to exploit the new opportunities provided by computers. We may choose to use computers to assist the individual in his daily activities, or we may choose to use computers as organizational tools aimed at gaining better control over the individual" [10].

If society is to avoid this polarization, it must take positive actions to effect constructive influences on the development of technology. For the computer utility to evolve, it must be general purpose enough to create sufficient demand for its services.* It is the prevalence of remote access terminals that provides the vehicle for mass participation in the operations of society. For example, it is considered an important protection of individual rights to be able to call one's lawyer when arrested. Note, there is an implicit assumption that one's lawyer has a telephone. In the same fashion, necessary protections such as the ability to control access to information about one's self and the ability to ensure its accuracy, are quite impotent unless the mechanisms for remote access are readily available and easy to use.

---

*To minimize the overhead costs of consoles, transmission lines, etc., the utility must offer a multitude of services (e.g., newspaper, catalogs, library, market research, and so on) in addition to satisfying its fundamental need to exist as an implementation of the properties derived above.

XI. SUMMARY

Through the computer, society can, if it wishes to, both restore the individual rights and obtain efficient operation. To succumb to the "efficiency syndrome" would be an irreparable error. Let no one think that the properties derived:

1) Control of access by the individual;

2) Accuracy and completeness of information;

3) Audit trail;

4) Potent legislative support

are anything less than absolute necessities. History, philosophy, and morality have proven these to be essential. Surely no one would consider buying an automobile without brakes; it is natural to have to stop periodically. If personal-information systems are allowed to proliferate, when society sees the red light ahead (*crisis*), there will be no brakes (*irreversible process*).

To secure the future existence of equality and freedom, society must create an environment that will force the evolution of the computer utility.* Unless computing power is *distributed uniformly* to all the people, via the general-

*"It is obvious that the political system in each society will be a fundamental force in shaping its balance of privacy, since certain patterns of privacy, disclosure, and surveillance are functional necessities for particular kinds of political regimes. This is shown most vividly by contrasting privacy in the democratic and the totalitarian state. The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups" [2].

purpose computer utility, the few that do control it (e.g., organizations--government) will be thereby endowed with disproportionate amounts of power. Physical proximity is no longer the critical factor affecting man's ability to compile information. Today's computer networks, communicating via telephone lines, are tantamount to centralized data banks:

> Like the problem of nuclear warfare, it is a time to reflect on how far we have come before we drift into a course that is beyond our capacity to navigate [23].

PART II

MEDICAL INFORMATION SYSTEMS AND THE PROTECTION OF PRIVACY

I. INTRODUCTION

The computer offers mankind the opportunity to exercise more effective control over his environment through its ability to handle large amounts of information both accurately and speedily. If put to proper use, information could be disseminated to the right people at the right time. In terms of biomedical information, the benefits to mankind would be two-fold:

1) The availability of timely and complete information concerning relevant aspects of an individual's case would greatly enhance his treatment;
2) Statistical uses of data on patients' treatment programs would be a tremendous boon to the fields of medical research, education, and drug control.*

This same computer ability, which promises to provide society with more efficient use of biomedical information, demands the most carefully conceived control mechanisms to prevent potential abuse of this information. This second part of this thesis applies the properties of safe information systems derived in the first part to problems currently encountered in the medical environment. Suggestions are presented for using available techniques to safeguard society's attempts at using the new information handling technologies (computers).

---

*Statistical information includes sample sizes of one, provided that anonymity is retained.

II. AN INFORMATION SYSTEM

In order to analyze the problem of privacy (or how to build an information system that will not do more harm than good), it is prudent to model the total system.* The components of this system (Fig. 3) are:

1) Data Base (*owner* of information);
2) Users;
3) Management;
4) Technology.

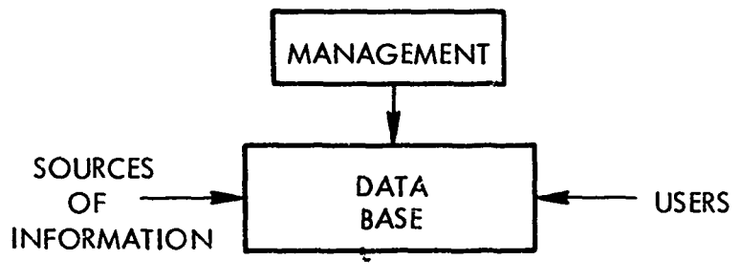

Fig. 3--A Medical Information System

The data base is comprised of information that is of *value* to both the owner and to society. For example, the chemical composition of a household item is valuable information to the firm that owns it (primarily in an economic sense). Protecting secrecy of the formula may be its best means of

*Analyzed in Part I.

maintaining a competitive advantage. However, to the mother whose child accidentally ingests a quantity of that product, information concerning the proper treatment is immeasurably valuable. The necessity is for some means of disseminating vital information while not sacrificing the rights of the owner. Thus, there exists a need for *mechanisms to control* the sharing of information in today's society.

In a personal context, information comprising an individual's medical history is highly sensitive and its confidentiality is of great value to the individual. Concurrently, that part of the record not concerned with personal identity is of significant value to the field of medicine in education, research, drug information (therapeutic effectiveness, contraindications, interactions, side effects), etc. Although it may be of no medical or social value to know that the particular history under examination is that of *John Doe*, it may indeed be of nefarious value to have that identifying information [17]. Again, the basic need to provide a capability for the *controlled sharing of information* is demonstrated.

In Fig. 4, a data base is modeled both as a set of facts and a set of relations operating on those facts. In existing information systems, relations between facts are often implied by physical proximity. Names and addresses appearing on the same forms are assumed to go together. Similarly, within a computer an address following a name is assumed to

be related. This phenomenon of *implied* relation becomes most critical when viewing the role and resultant potential threat to privacy of the *management* of a medical information system. For instance, if they have the ability to *control* a machine through *hardware*, a straight dump onto paper could reveal much supposedly confidential information.

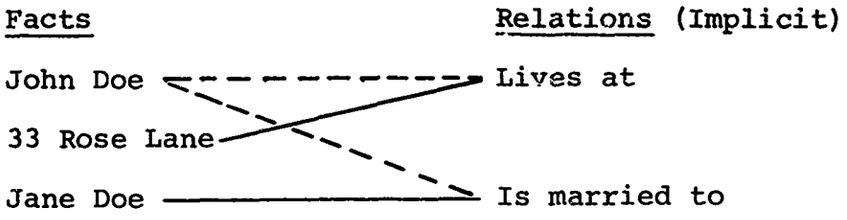

Fig. 4--Model: A Data Base

Vis à vis the protection of privacy, the most important characteristic of the management of an information system is management's potent ability to access the data base coupled with their utter lack of permission to do so. Their sole responsibility is to insure efficient operation of the facility; the actual content of the data base is irrelevant to the performance of their duties. Therefore, adequate safeguards must be intrinsic in the system (technology) to minimize the danger of compromise at this level.

A TOXICOLOGICAL INFORMATION SYSTEM

For a patient's records, medical-data base (personal information), or a poison-control data base (proprietary information), there exists a spectrum of users whose need to access the information system varies. Using the model of an information system (see Fig. 3) developed in this Paper, the basic functions and operations of the system will be outlined.* Users of the information contained in this system vary from the layman who has an immediate need for certain advice (e.g., "do not induce vomiting" or "lie down quietly," etc.), to the research pharmacologist or biochemist who is attempting to discover new and better antidotes for these toxic agents. Somewhere in the middle are practicing physicians and medical students interested in educating themselves on toxicology and the latest therapeutic techniques.

It would be desirable to design a dynamic system, actively involved in coordinating efforts to devise better antidotes, test them, and eventually incorporate them into common practice. This facility would naturally be useful to those industries involved in producing toxic items.

A DRUG INFORMATION SYSTEM

According to Goodman and Gilman in their standard textbook on therapeutic pharmacology:

---

*See Appendix.

> *A drug is broadly defined as any chemical agent that affects living protoplasm. . . . Primarily the physician is interested only in drugs that are useful in the prevention, diagnosis, and treatment of human disease, or in the prevention of pregnancy* [24].

The most common cases confronted by a doctor concerning drugs are:

1) *Prescription:* Prescribing a drug for a patient based on his current problem (disease), or past history (allergies, diseases, etc.).
2) *Poisoning:* Treating a patient who has ingested an overdose of one or a combination of drugs.

In order to deal with these problems successfully, a doctor must have an information source available that is accurate, timely, and complete.

The poison control *network* has been created to meet such a need in the event of overdose or accidental ingestion. However, there is still much to be desired in an effective information system to satisfy the first case.

COMPOSITION OF INFORMATION

The ideal drug information system would be comprised of a data base that would objectively provide accurate and complete information at the time it was required. In order to analyze the privacy considerations of such a system, one must first define that set of information necessary for saving lives through the proper use of drugs (and antidotes).

The next step is to identify those items of information that may be considered proprietary. The resultant system

design must then integrate the goals (timely information) and the constraints (controlled dissemination) into a workable facility.

A PROPOSED INTEGRATION

An interview with Miss Francis Weindler, R.N., Director of the Los Angeles Poison Control Center (LAPCC) at the Children's Hospital, has disclosed that the information necessary to save human lives as a result of poisoning is, in the final analysis, available. There was some difficulty in acquiring crucial information from companies at the outset, but now that most are familiar with the LAPCC's function, method of operation, and integrity, they appear willing to cooperate.

A discussion with an M.D. who runs a small, private biochemical analysis laboratory also confirms the availability of information to *qualified personnel*. A major drawback, however, is the time factor. It is often impossible to retrieve information when it is critically needed.* Months may elapse between the time certain information (e.g., the active agent of a drug) is both requested and received.

---

*A child, for example, has ingested an unknown poison. Given that one suspects a particular substance (based on symptoms or partial information offered by the parents), one must test for its presence. The test methodologies suggested by drug companies to detect the presence of their products are often inefficient, laborious, time consuming, or unavailable. It is not uncommon to be forced to devise one's own test on the spur of the moment. Needless to say, failure to identify a toxic agent immediately has cost numerous lives.

THE PRESENT PROBLEM

Today's methods of drug development, testing, and release leave much to be desired in terms of protecting the public from harm due to incomplete and inaccurate drug information available to doctors.

> For example, the Food and Drug Administration employs only a single physician to conduct field investigations of all the studies underway in the United States, and the agency's inquiries rarely go behind the dry scientific data . . . 'Our responsibility is not the direct supervision of the [drug] investigators,' FDA Commissioner, Dr. Lay, said in an interview [25].

The availability of *objective* and *current* information concerning the performance (therapeutic value) and hazards (side effects, contraindications) of drugs is alarmingly deficient. Primarily responsible for this shortcoming is the *open loop* nature of the present system. What is needed is a feasible and effective closed loop system. Dr. H. Moshin, of The RAND Corporation, is completing work concerning the design of a new drug testing and evaluating system (Fig. 5). The basic philosophy can be summed up in this statement by Senator Gaylord Nelson:

> *Testing of drugs should be done by specialists who have no direct relationship with manufacturers, who cannot benefit financially from the results, and who are not motivated even subconsciously by the desire to get anything but the truth* [26].

This is a closed loop system that, through the independent organization of specialists, fulfills two critically important functions:

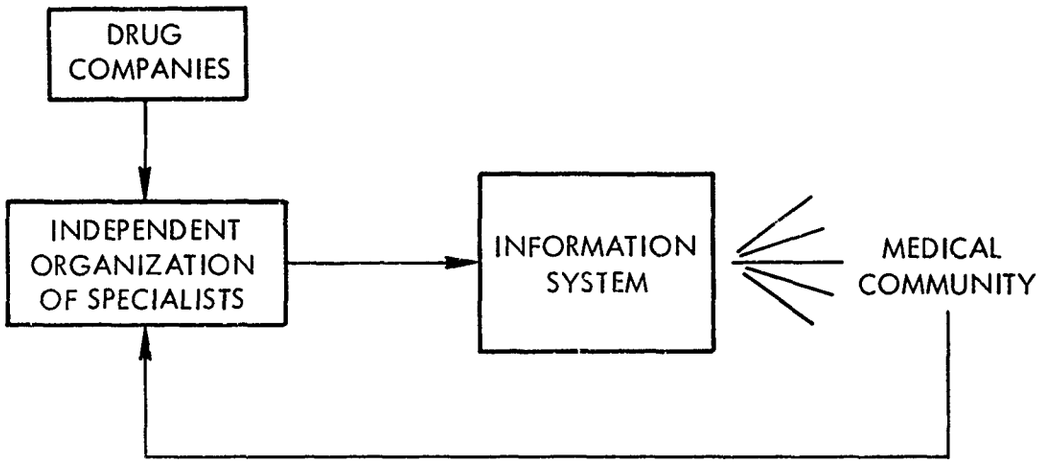

Fig. 5--A New Drug System

1) It performs objective tests on drugs and compiles a complete set of vital information to be initially entered in the Information System.*

2) It provides a feedback mechanism to enhance the accuracy and completeness of initial tests of drug performance through the monitoring of actual performance on the general public.† In this capacity, the independent organization is expected to obtain, process and verify data on the performance of drugs in the public area. It, then, is responsible for updating the information system accordingly.

---

*In this capacity, the information system would function as an idealized extension of the *Physician's Desk Reference (PDR) to Pharmaceutical Specialties and Biologicals* [27].

†Each time a drug is used, information concerning its therapeutic effectiveness is generated. A convenient mechanism (multi-access *information system*) must be built to gather this information to be subsequently processed by the independent organization of specialists, and then released to doctors (capacity 1) via the information system.

III. THE PATIENT'S MEDICAL RECORD

In the early days of medicine, the family doctor was part of the family. It was not uncommon for him to pay house calls, even in times of health, merely to check on his patients and eat dinner with them. Often, he knew his patients since birth. When they were ill, he would visit them at their dwellings. With only a few drugs available, it was quite easy for the doctor to remember each patient's history and reactions. At most, records were fragmentary.

In today's world, however, a number of factors have modified the doctor-patient relationship.

> Ben Casey and Dr. Kildare notwithstanding, the modern-day physician, in the public's image, seems not to be the equal of his counterpart of fifty years ago. Where once the doctor was the warm, friendly constant family attendant from the birth of his patients onward, the modern physician--or so goes the complaint--is a specialist seen only for special needs, often too busy for house calls, who treats patients with the cold efficiency of an assembly-line foreman [28].

Combined with the medical ethic of treating the *whole man*, these phenomena have necessitated the keeping of comprehensive records:

1) *Complexity:* The *knowledge explosion* in medicine has been formidable. There are well over 2000 drugs on the market, most with very special therapeutic uses, manifold side effects, and contraindications [27]. In fact, it has become so complicated that new concepts of medical care involve health *teams* where one

member is a clinical pharmacologist who acts as the consultant on drugs [28].

2) *Specialization:* A natural consequence of complexity is the need to specialize. There is so much known in any single area that in order to become proficient, one must devote all one's time to that area. The so-called *specialists* only see patients on referral. As a result, they are even further removed from the patient's identity.

3) *Population:* The population increase has resulted in exerting extreme demands on a doctor's time; a house call today is a rare occurrence. This is almost universally true in urban centers. The intimate relationship between doctor and patient in these urban centers is a myth of the past era. In metropolitan hospitals, doctors see patients for short intervals, perhaps once in each person's life.

4) *Mobility:* The mobility of our society is unprecedented. Vast numbers of students go away to school; families continually relocate to follow job opportunities. A natural consequence of this mobility is further destruction of the old doctor-patient relationship.

A RESUME

What needs to be appreciated about modern medicine is that increased specialization has been the inevitable

> result of the great scientific strides in medicine during the past half-century, and that this scientific progress rests more solidly on humanitarianism than does the venerated 'bedside manner.' Moreover, doctors nowadays are no less concerned with the general comfort and health of patients; they strive to treat the 'whole patient,' but wisely prefer to limit their counsel and treatment to the areas in which they have been well-trained [28].

It is apparent that some mechanism for filling the void created by complexity, population, and mobility is mandatory. It must introduce the *whole patient* to the doctor in real time. In short, it must be a compendium of the medically relevant aspects of the patient as an *individual* (i.e., social environment, psychological composition, etc.) and as a medical specimen (e.g., complete disease, drug and allergy history). This is the primal function of the patient's medical record.

WHO OWNS THE MEDICAL RECORD

The medical record is a problem-oriented diary of an individual's life, *designed to facilitate communication between a doctor and the patient*. It serves to fill in necessary details that, due to complexity, cannot be remembered (by the doctor or the patient). This record depicts a portrait of the patient as an individual human being, as objectively and professionally as medical personnel are capable of recording [29].

Recognizing that: 1) the individual is ultimately responsible for his own well being; and 2) the medical record is the individual's compendium that is specifically designed to facilitate the delivery of medical care, it follows that the

medical record itself should be the sole property of the individual described.*

Since the medical record is information about an identifiable individual, the controlled dissemination of that information belongs to the individual therein described. Retention of this control affects information given in confidence. In other words, when you tell a doctor something *in confidence*, it is *not* his prerogative to divulge that information [20].

USES OF THE PATIENT'S MEDICAL RECORD

Effective practice of medicine demands certain information in a patient's medical record be made available for professional uses. These needs include case histories for education--both undergraduate and continuing, and constructing valid models for medical analysis, etc. Also, in order to evaluate the performance of drugs (therapeutic value, side effects, interaction incidences), it is often necessary to have a fairly complete medical history available. Thus, while the patient's medical record is of vital importance to him, it is also of value to society. A system must be designed whereby needed information is made available while the individual's right to privacy is guaranteed.

---

*There may be some question as to the wisdom of allowing a patient to read his complete medical record. However, it is by no means obvious that he should not be able to see it, if he so desires [16].

PROPERTIES OF SOCIALLY USEFUL MEDICAL INFORMATION

An outstanding property of socially useful medical information is that it need not contain any individually identifying information such as a name, number, address, etc.* A history of drug use for the Drug Information System makes no use of individually identifiable data; neither would a case history presented to medical students.

The only instance that would require identifying information would be the monitoring of a patient's progress over time. In that event, however, the patient must be aware of the need and must have given his consent [19].

Thus, the need to correlate medical history with an identifiable individual is primarily of use to that individual. He (the patient) is able to benefit from comprehensive and accurate records regardless of with what doctor or hospital he may find himself as a result of an emergency (or of free choice).

---

*In the incidence of certain contagious diseases, it may be argued that identifying information is a necessity for treatment and prevention of contamination. But, these cases can be adequately handled following the guidelines developed in this Paper. Only specific authorities, commissioned with containment of certain diseases, need be aware of identity; likewise, only the patient's doctor need be advised of *all* the facts.

IV. PRESENT TECHNOLOGY

An information system designed to protect the privacy of individuals whose information comprises the data base of the system must satisfy certain basic requirements. These properties, discussed in Part I, are:

1) *Control of Access by Individual;*
2) *Accuracy and Completeness of Information;*
3) *Audit Trail;*
4) *Potent Legislative Support.*

This section offers a suggested implementation in terms of today's technology. A clear statement of present limitations and what effect they have on the power of the system is presented. A prognosis will be advanced to advise directions for further development.

ACCESSIBLE COMPUTING

Today, it is impossible to provide an effective, technically implemented (hardware/software) facility to enable an individual to control access to his file. It is thus necessary for him to rely on other people to protect the integrity and secrecy of his information, an extremely significant liability in an information system. Consequently, certain constraints must be placed on personnel and content in order to protect the rights of the data base owners [30,31].

In view of this vulnerability, the following recommendations are offered to minimize the probability of compromise:

1) *Design Modular Systems*--which would enhance certification of protection mechanisms. It would also localize (*containerize*) sensitive programs to feasibly subject them to close scrutiny.

2) *Minimize Temptation to "Break" System*--Mechanisms (*technical*) must be incorporated in the initial design of these systems to insure that the cost of compromising the system would be far greater than the value of the information obtained by said action [see Eq. (1), Fig. 6]. Also, the cost of protecting this information must be less than its value [see Eq. (2)]. Note that "value" is subjective and therefore hard to determine (refer to discussion in Part I).

$$C_v >> V_{Iv} \qquad (1)$$

$$C_p << V_{Io} \qquad (2)$$

C_v = Cost of Violating System

C_p = Cost of Protecting System

V_{Iv} = Value of Information to Violator

V_{Io} = Value of Information to "owner"

Fig. 6--System Protection Costs

The more sensitive the information, the more resources must be expended to protect it. Alternatively, if a certain

level of protection cannot be guaranteed, the information contained must be correspondingly limited in value.

IMPLICATIONS ON SYSTEM CONTENT

It must be argued that, ultimately, one has to trust others to be honest. Even in a remote access system with terminals readily available, one is forced to assume the system is indeed obeying one's requests *and* nothing else. This also assumes that the operating personnel, systems programmers, *et al.* (those that have intimate and powerful control over the computer system) are, at the very least, unscrupulously honest.

As H. Petersen and R. Turn conclude:

> *Trustworthy and competent personnel will establish and maintain the integrity of the system hardware and software which, in turn, permits use of other protective techniques* [31].

The critical vulnerability in an information system employing privacy protection mechanisms is the management of the system (see Fig. 3). In accordance with the following design philosophy,

> It is easy to be honest
> when you are not presented with
> a good opportunity
> to be dishonest.

It is strongly recommended that the information content of any system be as limited in scope as is possible to provide a useful service while not presenting a dangerous temptation (vis à vis *the management*) to violate the system.

Existing computer systems are subject to frequent breakdowns resulting from both hardware and software malfunctions. It is not uncommon, in these instances, for files to become erased, misplaced, or moved to another location wit changed access rights. A contributing factor in these malfunctions is the present difficulty in debugging, and therefore certifying, the behavior of large programs. Constant preventive maintenance (another requirement of today's systems) only serves to amplify the present dependency on system personnel and increase system vulnerability to sophisticated attacks.

A LACK OF EXPERIENCE

There is a conspicuous lack of experience in designing and implementing privacy systems on computers [30]. Only the most rudimentary techniques have been operating in today's computer systems. Fundamental hardware/software mechanisms, such as bounds registers, dual modes of operation (master and slave), etc., have been necessary just to keep an operating system in a multiprogrammed (and time-shared) environment functioning.

Software protection mechanisms, such as passwords, have been only moderately successful.* However, it is imperative to realize that many of the weaknesses in present systems (such as those in CTSS at MIT) [17], have been discovered only through years of use.

---

*One-time-only passwords, however, offer much greater protection than multi-use ones.

V. RECOMMENDATIONS FOR AN IMPLEMENTATION

A sophisticated and powerful tool has been created by man that enables him to effectively handle vast amounts of information. This section discusses the issues involved in creating a useful, *computerized*, medical information system. In so doing, it replaces certain current myths with a realistic understanding of the nature of present constraints.

It has been said that locks are for honest people. No protection mechanism exists that cannot be broken; however, different levels of protection do exist. The critical variable is cost:

1) What costs are incurred by the invader attempting to compromise a particular system?
2) What value can the invader accrue as a result of successful compromise?
3) How much are you willing to pay to protect the system?

There are certain functions of a protection mechanism that, in order for it to be effective, demand implementation. They are: prevention and apprehension.

If it were possible (which it is not) to guarantee that either a *prevention* facility or an *apprehension* facility was 100 percent effective,* it would be necessary to build only one *or* the other to *guarantee* adequate protection. In the first case, any attempted invasion would be a failure,

*The ratio $C_v/\cdot V_{Iv} \rightarrow \infty$, see Fig. 6.

regardless of the resources expended by the would-be intruder. In the latter, regardless of what compromise was experienced, the intruder would be caught and punished. However, since neither facility is foolproof, it will be shown that a mixture of *both* a prevention mechanism *and* an apprehension mechanism is necessary to provide adequate protection.

PROTECTION FUNCTIONS

Information, unlike material objects, can be *stolen* (duplicated) while remaining *untouched*.* The very nature of information places significant demands on a protection mechanism. If attempted espionage cannot be prevented (failure of prevention mechanism), it is *mandatory* that it be detected. Failure to prevent *and* notice a theft naturally results in a failure to apprehend. Therefore, a prevention system must serve 1) to prevent unauthorized access to information, and 2) to record all attempts to access information, successful or not, as an aid in apprehending violators of system integrity.†

Two audit trails must be maintained to provide an effective apprehension facility. The first, controlled by the prevention mechanism, would record information such as name,

---

*On a computer, when one reads a file, one does not modify it. In a non-computer sphere, any information can be photo-duplicated without raising suspicion, provided the original is returned intact to its most recent location.

†An *audit* system should function within the framework of a prevention mechanism to gather for future analysis as much data about the intruder as is possible.

date, time, file to be referenced, purpose, and success. The second audit trail would be maintained by the Operating System. It would record the name of the file, data, and time opened. The two audit trails could then be compared for mismatch, thereby reducing the probability of an undetected violation of the system.

PROTECTION DESIGN

The mechanisms necessary to prevent the unnecessary and perhaps undesirable dissemination of information in a system such as this are:

1) Ability to restrict access to information (Prevention Facility). That is, the ability to *verify* who is asking for information, what their need is, and then answer with only the information necessary to complete the approved task.
2) Maintenance of an audit trail (prevention *and* apprehension function). This record would be useful to enable enforcement of the restricted access facility.
3) A new legal structure* (prevention *and* apprehension):
   a) to force the creation of a *safe* system;
   b) to enumerate those acts specifically outlawed;
   c) to hold *each individual accountable* for his actions;

*"Do not expect help from the legal profession *in lieu of good design*" [12].

d) to perhaps *review* present *patent* and *copyright* laws in view of apparent inadequacies, to both protect the *owner* of an *idea* and at the same time protect the public from the consequences of imperfect knowledge concerning the use of the *idea*.

IMPLEMENTATION

A variety of factors affect the adequacy of protection a system can provide. A preferred situation would be the design of (prevention/apprehension) mechanisms that defy compromise. They would protect against passive (tapping, etc.) and active (illegal access, impairment of service, etc.) attempts at compromising the system. However, since the present technology cannot guarantee a safe system via omnipotent technological protection, the value of the information contained in the system must be correspondingly adjusted (see Fig. 6).

Adequate protection involves a mixture of procedural and technical designs:

1) Individual clearances (management function includes maintenance personnel, refer to Part I, p. 20);
2) Certification of system storage;
3) Encryption of data in storage;*

*Enough to obscure the meaning.

4) Storage of data *randomly* to avoid contextual interpretation (*implied* relations)--see Fig. 4;

5) Decentralize hardware control in such a manner that compromising the system would involve a conspiracy (Fail-Safe operation);

6) Core and drum areas should be zeroed before handing to user;

7) *Complete instruction decoding*, to prevent execution of illegal (and unpredictable) instructions;

8) Partition--hardware separation of supervisor functions and user areas;

9) Lock the computer room;

10) Time delay on errors--to prevent *iterative* attempts at breaking down prevention mechanism. Note that the audit trail will provide some delay *and* record each iteration to aid in *apprehension*;

11) Input and output via *protected* buffers;

12) Careful checking of all I/O requests.

VI. FUTURE DEVELOPMENTS

Privacy protection mechanisms in computer systems are non-analytic. At present, exhaustive enumeration appears to be the only method for designing, implementing, and testing (certifying) these systems. More experience with these facilities is needed, through use *and* monitoring, in order to develop a methodology for accurately certifying the privacy protection mechanisms operative in any given system.

The proper environment for this learning process is one in which the event of failure is both instructive and non-disastrous, specifically:

1) Information content is limited in scope to decrease possible temptation for systems personnel to *steal* it.

2) All users and operators are of high caliber, cleared, and fully cognizant of the *experimental* nature of the system.* In the event of a failure of the protection mechanisms, they will:

   a) report it--to aid in diagnosing the problem;

   b) destroy or return any information divulged as a result of the malfunction, eliminating the possibility of actual damage.

---

*Based upon the preceding discussion, it is clear that any system, in use today or the near future, is by definition experimental.

Throughout this experimental stage, a group of experts will be continually attempting to violate the system.* Eventually, techniques for protecting the integrity of the information contained in the system would be developed that would be both dependable and certifiable.

---

*In order to guarantee sophisticated and determined attacks, one might offer a bonus of, say, $100 for each successful violation. Receipt of this reward might be contingent upon a design for preventing it, too. One might find college students to be particularly industrious in this role!

VII. SAFE MEDICAL INFORMATION SYSTEMS

Following the recommendations given in Sec. VI, it is feasible to implement secure medical information systems. A drug (*and* toxicological) information system would be a computerized version of the PDR [27] and the LAPCC. Its services, however, would be available nationwide.

In this initial design, the only personnel granted access to this information system would be *friendly** and cleared. Only doctors would be allowed to query the Center.† A complete audit system would be maintained (as is now done at LAPCC (see Fig. 7). This further serves to discourage nefarious attempts at intrusion as it *fully* documents each call. In addition, in questionable cases, hang-up and call-back procedures would be used by the nurse on duty.

In this manner, an *effective* toxicological information system will be developed concurrently with secure (certifiable) protection mechanisms. It may then prove feasible to supply hospitals with remote access terminals to make important information even more readily available‡ [31].

A similar design may be implemented for patient's medical records. Again, a fairly secure system can now be built

---

*In the manner described in Sec. VI.

†This serves two functions: 1) discourages fradulent attempts to access the information system; and 2) forces the public to seek professional help in the event of poisoning.

‡The possibility of active or passive violation of the system via tapping communications can be virtually eliminated through excryption of the transmission [32].

Call From

THOMAS J. FLEMING MEMORIAL
POISON INFORMATION CENTER

MONTH

INITIAL REPORT

CHILDRENS HOSPITAL OF LOS ANGELES

Doctor or Hospital

Lay Person

Date _____ 19____ Time call rec'd _____ AM PM

TRADE NAME _____

Manufacturer Address & Phone _____

Ingredient _____

Amount Ingested _____ Check if Amt. Unknown ____ Inhalation ____ Eye and/or Skin Contact ____

Lavaged Yes No Vomited Yes No Check if Over a Period of Time _____ Time of Contact _____ AM PM

Signs & Symptoms _____

Why? Accident - Industrial - Suicide - Info Only - Explain if necessary _____

Pt. and/or Parent's Name _____ Age _____ Mos. Yrs. M F

Name (if info) _____ Adult (if over 21)

Address & Phone _____

DOCTOR _____ / _____ Phone MUST be given

Address _____ / _____ City

Info given & source _____

(OVER IF NECESSARY)

R.N.
_____ _____ M.D.
SIGNATURE

Fig. 7--Poison Information Center--Initial Report

given the unquestionable virtue of the management (operators, systems programmer., engineers, and their administrators). This facility could be started on a *local* basis with two audit trails maintained. One would document completely each request for information on identifiable individuals, while the second would be a record of authorizations (by signature) of the individuals concerned.

This information system would be experimenting with restricted access mechanisms that would eventually (if proven safe) allow on-line access to a spectrum of users with varying needs and access rights (see Fig. 3)

VIII. CONCLUSIONS

The trend towards the agglomeration of data on individuals, via the computer, presents a serious threat to the individual's right to privacy. If allowed to proliferate, the deleterious effects on the individual, and therefore society, are likely to be irreparable. Because of *the momentum of technology* and the *irreversibility* of social processes, Society must act immediately if it is to ensure the evolution of "safe" information systems. An environment must be constructed that preferentially fosters the development of desirable systems.

The very nature of information makes the price of failure prohibitive. Once "stolen" (revealed) it can never be returned; nor can the resultant damage be objectively valued. On the contrary, the value of personal information to the individual concerned is by definition subjective. Therefore, properties providing the individual his rightful control over the dissemination of personal information must be inherent in any personal-information system.* These are:

1) *Access Control:* The *owner* of the information specifies who may access it, under what conditions, and what they are privileged to see.

---

*The implementation of these properties requires the existence of a suitable mechanism, such as the availability of terminals, in the same way the right to call your lawyer presumes the availability of telephones.

2) *Accuracy and Completeness of Information:* The individual must be protected against damage by false or misleading information. This protection mechanism implies a broad invulnerability of the system to *tampering*. To check (verify) the status of information about him, the individual must be able to access the data base and know he has seen the *entire* contents. A third party (review) mechanism must be created to adjudicate disputes regarding the truth of the information stored in the system.

3) *Audit Trail:* The system must maintain a complete record of who attempted to access a file, the reason, and the result of the inquiry. In addition, a mechanism must exist whereby the individual is kept abreast of the activity of his file. This satisfies the requirement that the individual know at all times who knows what about him.

Realizing that "Real protection in this world comes not from people's good intentions, but from the law" [16], it follows that a package of legal controls must be legislated. This necessary *Legal Environment* should establish a statutory right to privacy that cites attempts to compromise the integrity of the information system as criminal acts. Employees should be held individually accountable for their actions. Finally, systems not possessing the proper technical properties should be enjoined from continuing to operate.

The philosophy embodied by these properties are meant to guide the evolution of technology, not be obsoleted by it. In that respect, they are implementation independent. Today, for example, information could be classified into groups and *Access Control* legislated in much the same way that defense classified information is handled. There are, however, fundamental and important differences between the problems of handling defense classified information and personal information. They lay in the area of the subjective determination of value based on man's individuality.

Although recognizing that the computer utility is perhaps 30 years from implementation, this thesis argues that society must force the evolution of widespread, distributed computing power if man is indeed to live as an individual rather than a *1984* humanoid. Using available safety measures such as legislation, clearances (since we must in fact "trust" the system's personnel), the Postal System (Audit Trail notifications), and limitations on centralization of information (reduce the temptation to violate the system) society should be able to weather this interim evolutionary period.

APPENDIX

A FRAMEWORK FOR SYSTEM IMPLEMENTATION

Fig. 8--Medical Records*

It is useful to view the system of Fig. 3 as one with users that can *Read Only*, other users that can *Read/Write*, and still others that can *Write Only*. Thus, we can enumerate the uses of such an information system thereby grasping a hold on the privacy problem.

Most of the users who have the ability to *Read Only* would be interested in the clinical history from either a research or education-oriented point of view. Any information that would divulge the specific identity of the individual under observation would not be necessary. Also, standard programs might exist that would scan the data base periodically to maintain accurate statistical data concerning drugs and drug use (therapeutic effectiveness, contraindications, correlation with disease occurrences, interactions), and disease information (incidences, correlations, treatments that are

*Arrows depict flow of information.

interlinked such as: how should the *standard* treatment of disease A change because of the presence of disease B [simultaneously or in the past]).

There also will be a group of users in a *Read Only* category that would require the ability to investigate medical histories of identifiable individuals. These might be insurance companies interested in investigating the feasibility of granting life and/or health insurance, and corporations who normally request medical records, etc. However, it is not clear that either of these sources *need* medical information in as fine-grain detail as exists in the medical record. Again, perhaps some program could scan the record and compute an answer to present to the insurance company. In other words, a system that would divulge only as much information as was necessary to enable society to function smoothly while not excessively infringing on the individual's privacy. For example, the fact that an individual visited a psychologist to discuss certain psycho-sexual matters is an unimportant detail concerning his health insurability. However, his having a heart condition would definitely be significant.

Those with a *Write* capability obviously have the power to affect the status of an individual's record; however, depending on functions, it is limited and specific. For example, a laboratory may be able to *Write* the results of a series of tests into a patient's file, but in no way should they be

able to peruse this file.* The doctor, however, must have the ability to both peruse the entire record and modify and append information as circumstance dictates. The medical staff responsible for treating a patient must also have *Read* and *Write* access to the file.

---

*This may be accomplished via a certified system program. For example, the laboratory writes the results of a test (or series of tests) in a file called, say, Test. They then invoke a (privileged to the lab) system command to write this file (Test) into the file of *John Doe*. Before the system executes this command, however, it first checks to authenticate the identity (*individual* lab attendant) of the requestor, verify the identity of the patient through a doctor's request entry, confirm that the tests reported by the lab were those requested by the doctor, and record the transaction in an audit trail. It is not necessary for the laboratory to have the *actual* name of the patient they are dealing with, they only need *some* identifying property. A random number, for example, supplied by the information system could serve this purpose quite nicely. This further protects the individual from arbitrary abuses.

REFERENCES

1. Fried, Charles, "Privacy," *Yale Law Journal*, Vol. 77, No. 3, January 1968, p. 475
2. Westin, Alan, *Privacy and Freedom*, Athenum, 1967.
3. Warren, S. D., and L. D., Brandeis, "The Right to Privacy," *Landmarks of Law*, Henson (ed.), Beacon Press, Boston, 1963.
4. Westin, Alan, "The Snooping Machine," *Playboy*, Vol. 15, No. 5, May 1968, p. 130.
5. U.S. Congress, "Commercial Credit Bureaus--Hearings Before a Subcommittee of the Committee on Government Operations," House of Representatives, Ninetieth Congress, Second Session, U.S. Government Printing Office, Washington, D.C., March 12-14, 1968.
6. -----, "The Computer and Invasion of Privacy," Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives, Eighty-Ninth Congress, Second Session, U.S. Government Printing Office, Washington, D.C., July 26-28, 1966.
7. Fano, R. M., "The Balance of Knowledge and the Balance of Power," *Scientific American*, Vol. 218, No. 5, May 1968, pp. 149-152.
8. Laski, H. J., "The Personality of Associations," *Landmarks of Law*, Henson (ed.), Beacon Press, Boston, 1966.
9. Saloma, J. S., 3d, "System Politics: The Presidency and Congress in the Future," *Technology Review*, December 1968, pp. 23-33.
10. Fano, R. M., "The Computer Utility and the Community," *1967 IEEE International Convention Record*, Part 12, pp. 30-37.
11. Baran, Paul, *On the Engineers Responsibility in Protecting Privacy*, The RAND Corporation, P-3829, May 1968.
12. -----, *Communications, Computers, and People*, The RAND Corporation, P-3235, November 1965.
13. Selznick, Phillip, *Leadership in Administration*, Harper and Row, New York, 1957.
14. Zion, S. E., "Detective in Nader Case Says GM Altered Papers," *The New York Times*, February 5, 1967, p. 1, col. 2.
15. Long, Edward, "Big Brother in America," *Playboy*, Vol. 14, No. 1, January 1967.

16. Curran, W. J., *et al.*, "Privacy, Confidentiality and Other Legal Considerations in the Establishment of a Centralized Health-Data System," *The New England Journal of Medicine*, July 31, 1969, pp. 241-247.

17. Baran, Paul, *Remarks on the Question of Privacy Raised by the Automation of Mental Health Records*, The RAND Corporation, P-3523, April 1966.

18. Lickson, Charles P., "Privacy and the Computer Age," *IEEE Spectrum*, October 1968, p. 58.

19. Hilmar, N. A., "Anonymity, Confidentiality, and Invasions of Privacy: Responsibility of the Researcher," *A.J.P.H.*, Vol. 58, No. 2, p. 324.

20. "The Security Leak at the 1040 Level," *Business Week*, April 18, 1970, p. 32.

21. Gallagher, Cornelius, "A Letter to John L. Spafford--Special Studies Subcommittee of the Committee on Government Operations," Ninety-First Congress, U.S. Government Printing Office, Washington, D.C., March 21, 1969.

22. Armer, Paul, "Social Implications of the Computer Utility," *AFIPS Conference Proceedings*, August 1967.

23. Gallagher, Cornelius, "Science, Privacy, and Law--The Need for a Balance," *Proceedings and Debates of the Eighty-Ninth Congress*, Second Session, August 18, 1966.

24. Goodman, L. S., and A. Gilman, *The Pharmacological Basis of Therapeutics*, 3rd ed., The MacMillan Co., New York, 1965.

25. Rugaber, Walter, "Prison Drug and Plasma Projects Leave Fatal Trail," *The New York Times*, July 29, 1969, p. 1.

26. -----, "Senator Seeks a Federal Center to Take Over Testing of Drugs," *The New York Times*, July 30, 1969, p. 1.

27. *Physicians Desk Reference (PDR) to Pharmaceutical Specialties and Biologicals*, Medical Economics, Inc., 23rd ed., 1969.

28. *The Education of a Physician*, The Johns Hopkins University, Maryland, 1964.

29. Weed, Lawrence L., *Medical Records, Medical Education and Patient Care*, Case Western Reserve Press, 1969.

30. Ware, Willis, *Security and Privacy in Computer Systems*, The RAND Corporation, P-3544, April 1967.

31. Petersen, H. E., and Rein Turn, *System Implications of Information Privacy*, The RAND Corporation, P-3504, April 1967.

32. Baran, Paul, *On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations*, The RAND Corporation, RM-3765-PR, August 1964.

BIBLIOGRAPHY OF WORKS NOT REFERENCED

Ayres, B. Drummond, Jr., "Nader Knows What Makes the Wheels Turn," *The New York Times*, February 12, 1967, Sec. IV, p. 5, col. 1.

Baran, Paul, *Communication Policy Issues for the Coming Computer Utility*, The RAND Corporation, P-3685, May 1968.

Dennis, R. L., "Security in the Computer Environment," System Development Corporation, Santa Monica, California, August 18, 1966.

Forrester, J. W., "Common Foundations Underlying Engineering and Management," *IEEE Spectrum*, September 1964.

Hoffman, L. J., "Computers and Privacy: A Survey," *Computing Surveys*, Vol. 1, No. 2, June 1969.

Long, Edward, *The Intruders: The Invasion of Privacy by Government and Industry*, Praeger, New York, 1967.

"National Data Bank: Its Advocates Try to Erase 'Big Brother' Image," *Science*, Vol. 163, January 10, 1969.

Snedeker, Lendon, "On Confidentiality and Data Banks," *New England Journal of Medicine*, Vol. 281, No. 5, July 31, 1969, pp. 269-270.

Zion, S. E., "Ribicoff Seeking New GM Industry: He Raises Issues of Perjury Regarding Data on Nader," *The New York Times*, February 6, 1967, p. 1, col. 1.

-----, "GM Aide is Said to Assist Nader: Company Asserts Detective Helps in Private Suit," *The New York Times*, February 7, 1967, p. 2, col. 1.